

[0001]

[Technical Field of the Invention] The present invention relates to a personal information distribution management method for protecting personal information and activating distribution of information, in order to get authentication, conduct marketing and have necessary destination information when performing on-line shopping and electronic commerce, and receive personal services based on personal information, within an information distribution base in which a personal information possession subject who has at least one piece of personal information which can be disclosed and the personal information use subject who wants personal information to be disclosed from the personal information possession subject exist.

[0011] Referring to FIG. 1, the personal information distribution management apparatus which is an embodiment of the present invention is configured with the personal information input apparatus 1, the personal information registration section 2, memory and the secondary storage apparatus 3, the retrieval condition input apparatus 4, the personal information retrieval section 5, the personal information presentation section 6, and a display apparatus 7.

[0012] When there is personal information such as a name, an address and a birth date of which at least one disclosure is possible, a personal information possession subject edits these using personal information input unit 1, and in addition, creates disclosure conditions such as a use permitter, the use purpose and the disclosure range (step 11) for each item of personal information as a disclosure regulations. For example, "names are permitted to be disclosed to every people" and "addresses may be disclosed to OO, Inc. as long as it is used as the purpose of user support, however, the disclosure range is limited to the personal information use subject's organization" etc.

[0013] In the personal information registration section 2, a syntactic analysis is performed for the group which consists of inputted personal information and a disclosure use regulation, and the contents of a text described are read, and the information on the analysis result is registered in the secondary storage 3 which is a database (step 12). At this time, regarding personal information, an index which can search the values of each item of personal information and the items with a search key is created. Moreover, regarding disclosure use regulation, an index which can search disclosure objects such as items of personal information, a use permitter, the use purpose, the disclosure range, etc., is created.

[0014] Using the retrieval condition input apparatus 4, as shown in Table 1, the

personal information use subject creates the use purpose, the disclosure range, etc. as request use regulation for every item of personal information to be used and sends them to the personal information retrieval section 5 (step 13).

[0016] In the personal information retrieval section 5, the conditions of disclosure use regulation registered and the conditions of the request use regulation given as retrieval conditions are compared using an index and the group which consists of personal information and the disclosure use regulation which fulfill both conditions are searched (step 14).

[0017] At this time, when a plurality of personal information are defined in the disclosure use regulation for every different information use subjects and disclosure conditions, selected disclosure of personal information is possible. For example, it is possible to specify "for the people who works at the same company, disclose telephone number 1 as home telephone number and for the other people, disclose the telephone number 2" or "if it is for the purpose of user support, the mail address 1 will be disclosed as a work e-mail address and if it is for the purpose of sending out direct mails, the mail address 2 is disclosed and if it is for the purpose of obtaining profit, nothing is disclosed."

[0018] In the personal information presentation section 6, disclosed personal information is dynamically created based on a retrieval result by extracting the items of the personal information to be disclosed. In addition, for each item of the disclosed personal information, the use permission information is dynamically created based on disclosure use regulation and request use regulation. Then, the disclosed personal information and the use permission information are made into a group and managed and displayed on a display apparatus 7 (Step 15).

[0019] The use permission information is a use constraint which fulfills both conditions of the disclosure use regulation and the request use regulation which were mentioned above, and the items of personal information which are subject to use constraint, such as a use permitter, the original writer, the use purpose and the disclosure range, etc. are specified. Since the personal information obtained by personal information use subject is always managed as a pair with this use permission, an illegal use contrary to the intention of the original writer (personal information possession subject) can be restricted.

[0020] Moreover, when "redistribution of disclosed personal information" is permitted in the use permission information, a personal information use subject can turn into a personal information possession subject by inputting a new disclosure use regulation from the personal information input apparatus 1 within a range permitted by use

permission information.

[0021] In addition, a configuration such that a plurality of server sites which registered a set of groups which consist of personal information which can be disclosed and a disclosure use regulation exist in a dispersed state and that parallel transmission of the retrieval request to the server sites can be made possible.

[0022] Moreover, it is possible to acquire the disclosed personal information which can be redistributed from many personal information possession subjects registered in various server sites and create indexes, etc. within a range specified by the use permission information as a personal information use subject and provide services to inform which server site is the most efficient to ask for the requested personal information and carry out a retrieval to the other personal information use subject.

Personal Info. Indicator for Disclosure	Use Permitter	Use Purpose	Disclosure range
Personal Info. ID + Name	Arbitrary people	Unlimited	Redistribution possible
Personal Info. ID + Home Address	Other than $\Delta$ $\Delta$ Trading Co., Ltd.	User support	Your organization
Personal Info. ID + Home Phone No.	People in the same workplace	Individual use	Only you
Personal Info. ID + Work Phone No.	Arbitrary people	Marketing	Your organization
Personal Info. ID + Work E-mail Address	People in Or.jp Domain	Non-profit	Only you

[Table 1]

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-067323

(43)Date of publication of application : 16.03.2001

(51)Int.Cl. G06F 15/00  
G06F 17/30

(21)Application number : 11-238206

(71)Applicant : NIPPON TELEGR & TELEPH CORP  
<NTT>

(22)Date of filing : 25.08.1999

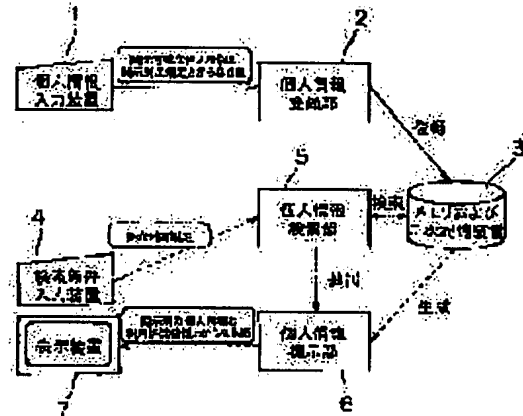
(72)Inventor : HASEGAWA TOMOHIRO  
TERANISHI YUICHI  
UMEMOTO YOSHIHIRO  
SATO TETSUJI

(54) PERSONAL INFORMATION DISTRIBUTION MANAGING METHOD, ITS DEVICE, RECORDING MEDIUM IN WHICH PERSONAL INFORMATION DISTRIBUTION MANAGEMENT PROGRAM IS RECORDED, INFORMATION SERVICE PROVIDING METHOD, ITS DEVICE AND RECORDING MEDIUM IN WHICH INFORMATION SERVICE PROVIDING PROGRAM IS RECORDED

(57)Abstract:

PROBLEM TO BE SOLVED: To restrict a subject to use personal information to use of it within a range permitted by use permission information.

SOLUTION: The personal information possible to be disclosed is edited, disclosure conditions are created as disclosure use regulation for each item of the personal information by using a personal information input device 1 by the subject to own the personal information. Syntax analysis is performed to a set consisting of the inputted personal information and the disclosure use regulation and its result is registered in a data base 3 by a personal information registering part 2. Request use regulation is created by using a retrieval condition input device 4 by the subject to own the personal information. A set consisting of the personal information to satisfy both registered conditions of the disclosure use regulation and the request use regulation and its disclosure use regulation is retrieved by a personal information retrieving part 5. Disclosed personal information is created based on a retrieval result, use permission information is dynamically created for each item of the disclosed personal information and the pieces of information are formed as a set and outputted to a display 7 by a personal information presenting part 6.



## LEGAL STATUS

[Date of request for examination] 12.10.2001

[Date of sending the examiner's decision of rejection] 23.03.2005

[Kind of final disposal of application other than

the examiner's decision of rejection or  
application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision  
of rejection]  
[Date of requesting appeal against examiner's  
decision of rejection]  
[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2001-67323  
(P2001-67323A)

(43) 公開日 平成13年 3月16日 (2001.3.16)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード <sup>*</sup> (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 Z 5 B 0 7 5
17/30		15/40	3 2 0 B 5 B 0 8 5
			3 7 0 Z

審査請求 未請求 請求項の数14 O L (全 7 頁)

(21) 出願番号 特願平11-238206

(22) 出願日 平成11年 8月25日 (1999.8.25)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目 3番 1号

(72) 発明者 長谷川 知洋

東京都千代田区大手町二丁目 3番 1号 日  
本電信電話株式会社内

(72) 発明者 寺西 裕一

東京都千代田区大手町二丁目 3番 1号 日  
本電信電話株式会社内

(74) 代理人 100088328

弁理士 金田 暢之

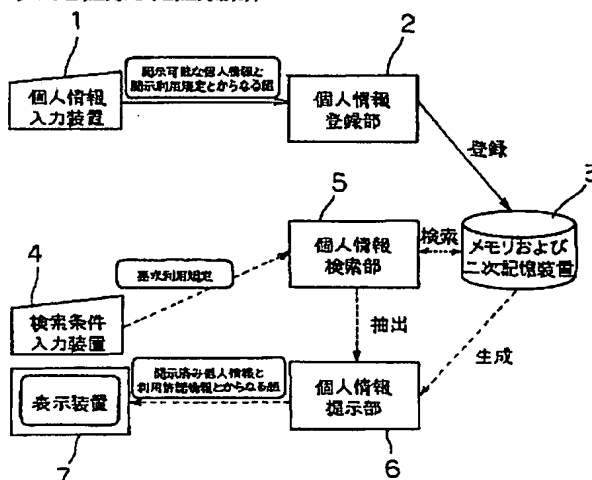
最終頁に続く

(54) 【発明の名称】 個人情報流通管理方法、装置、個人情報流通管理プログラムを記録した記録媒体、情報サービス提供方法、装置、情報サービス提供プログラムを記録した記録媒体

(57) 【要約】

【課題】 個人情報利用主体に対し、利用許可情報で許可された範囲内での利用に制限する。

【解決手段】 個人情報所持主体は、個人情報入力装置 1 を用いて、開示可能な個人情報を編集し、個人情報の各項目について、開示条件を開示利用規定として作成する。個人情報登録部 2 では、入力された個人情報と開示利用規定とからなる組を構文解析し、結果をデータベース 3 に登録する。個人情報利用主体は、検索条件入力装置 4 を用いて、要求利用規定を作成する。個人情報検索部 5 では、登録されている開示利用規定の条件と要求利用規定の両者の条件を満たす個人情報と該開示利用規定とからなる組を検索する。個人情報提示部 6 では、検索結果に基づき、開示済み個人情報を作成し、該開示済み個人情報の各項目に対して、利用許諾情報を動的に生成し、これらを組にして表示装置 7 に出力する。



**【特許請求の範囲】**

**【請求項1】** 個人情報とその開示条件を規定した開示利用規定との組をデータベースに登録する個人情報登録段階と、

前記データベースに登録された個人情報と開示利用規定とからなる組の集合に対し、検索条件として与えられる個人情報の利用条件を規定した要求利用規定に基づいて、開示利用規定と要求利用規定の両者の条件を満たす個人情報と開示利用規定とからなる組を検索する個人情報検索段階と、

検索の候補となった個人情報と開示利用規定の組と、検索条件として与えられる要求利用規定とに基づいて、開示済み個人情報と利用許諾情報を動的に生成し、前記開示済み個人情報と前記利用許諾情報を組にして個人情報利用主体に提示する個人情報提示段階とを有する個人情報流通管理方法。

**【請求項2】** 個人情報とその開示条件を規定した開示利用規定を作成する段階をさらに有する、請求項1記載の方法。

**【請求項3】** 前記利用要求規定を作成する段階をさらに有する、請求項1または2記載の方法。

**【請求項4】** 提示された利用許諾情報で規定された範囲内で新たな開示利用規定を規定し、開示済み個人情報と新たな開示利用規定とを組にして前記データベースに登録する段階をさらに有する、請求項1から3のいずれか1項記載の方法。

**【請求項5】** 個人情報利用主体に応じて異なる利用制約を規定した開示利用規定と個人情報利用主体が所持する開示可能な個人情報に基づいて個人情報所持主体の開示可能な個人情報を選択開示する段階をさらに有する請求項1から5のいずれか1項記載の方法。

**【請求項6】** データベースと、個人情報とその開示条件を規定した開示利用規定との組を前記データベースに登録する個人情報登録手段と、前記データベースに登録された個人情報と開示利用規定とからなる組の集合に対し、検索条件として与えられる個人情報の利用条件を規定した要求利用規定に基づいて、開示利用規定と要求利用規定の両者の条件を満たす個人情報と開示利用規定とからなる組を検索する個人情報検索手段と、表示装置と、

検索の候補となった個人情報と開示利用規定の組と、検索条件として与えられる要求利用規定とに基づいて、開示済み個人情報と利用許諾情報を動的に生成し、開示済み個人情報と利用許諾情報を組にして前記表示装置に表示する個人情報提示手段とを有する個人情報流通管理装置。

**【請求項7】** 個人情報とその開示条件を規定した開示利用規定を作成し、前記個人情報登録手段に入力する個人情報入力手段をさらに有する、請求項6記載の装置。

**【請求項8】** 前記利用要求規定を作成し、前記個人情報検索手段に入力する検索条件入力手段をさらに有する、請求項6または7記載の装置。

**【請求項9】** 個人情報とその開示条件を規定した開示利用規定との組をデータベースに登録する個人情報登録処理と、

前記データベースに登録された個人情報と開示利用規定とからなる組の集合に対し、検索条件として与えられる個人情報の利用条件を規定した要求利用規定に基づいて、開示利用規定と要求利用規定の両者の条件を満たす個人情報と開示利用規定とからなる組を検索する個人情報検索処理と、

検索の候補となった個人情報と開示利用規定の組と、検索条件として与えられる要求利用規定とに基づいて、開示済み個人情報と利用許諾情報を動的に生成し、前記開示済み個人情報と前記利用許諾情報を組にして個人情報利用主体に提示する個人情報提示処理とをコンピュータに実行させるための個人情報流通管理プログラムを記録した記録媒体。

**【請求項10】** 個人情報とその開示条件を規定した開示利用規定を作成する処理をさらに有する、請求項9記載の記録媒体。

**【請求項11】** 前記利用要求規定を作成する処理をさらに有する、請求項9または10記載の記録媒体。

**【請求項12】** 提供するサービスに必要な個人情報とその利用内容とに基づき、個人情報の要求利用規定を生成する要求利用規定生成段階と、データベースに登録された個人情報と開示利用規定とからなる組の集合に対し、前記要求利用規定に基づいて、前記開示利用規定と前記要求利用規定の両者の条件を満たす個人情報と開示利用規定とからなる組を検索する個人情報検索段階と、

検索の候補となった個人情報と開示利用規定の組と、検索条件として与えられる要求利用規定とに基づいて、開示済み個人情報と利用許諾情報を動的に生成し、前記開示済み個人情報と前記利用許諾情報の組を提示する個人情報提示段階と、前記開示済み個人情報と前記利用許諾情報からサービス利用主体に対しサービスの実行が可能かどうか判定し、可能であればサービス利用主体に対しサービスの提供を行うサービス提供判定段階を有する情報サービス提供方法。

**【請求項13】** 提供するサービスに必要な個人情報とその利用内容とに基づき、個人情報の要求利用規定を生成する要求利用規定生成手段と、データベースに登録された個人情報と開示利用規定とからなる組の集合に対し、前記要求利用規定に基づいて、前記開示利用規定と前記要求利用規定の両者の条件を満たす個人情報と開示利用規定とからなる組を検索する個人情報検索手段と、



検索の候補となった個人情報と開示利用規定の組と、検索条件として与えられる要求利用規定とに基づいて、開示済み個人情報と利用許諾情報を動的に生成し、前記開示済み個人情報と前記利用許諾情報の組を提示する個人情報提示手段と、

前記開示済み個人情報と前記利用許諾情報からサービス利用主体に対しサービスの実行が可能かどうか判定し、可能であればサービス利用主体に対しサービスの提供を行うサービス提供判定手段を有する情報サービス提供装置。

【請求項 14】 提供するサービスに必要となる個人情報とその利用内容とに基づき、個人情報の要求利用規定を生成する要求利用規定生成処理と、処理データベースに登録された個人情報と開示利用規定とからなる組の集合に対し、前記要求利用規定に基づいて、前記開示利用規定と前記要求利用規定の両者の条件を満たす個人情報と開示利用規定とからなる組を検索する個人情報検索処理と、

検索の候補となった個人情報と開示利用規定の組と、検索条件として与えられる要求利用規定とに基づいて、開示済み個人情報と利用許諾情報を動的に生成し、前記開示済み個人情報と前記利用許諾情報の組を提示する個人情報提示処理と、

前記開示済み個人情報と前記利用許諾情報からサービス利用主体に対しサービスの実行が可能かどうか判定し、可能であればサービス利用主体に対しサービスの提供を行うサービス提供判定処理をコンピュータに実行させるための情報サービス提供プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、オンラインショッピングや電子商取引を行う際の認証やマーケティング、配達先情報の必要性や個人情報に基づいた個人適応型サービスを受けるために、少なくとも1つの開示可能な個人情報を所持する個人情報所持主体と該個人情報所持主体から個人情報を開示して欲しい個人情報利用主体とが存在する情報流通基盤において、個人情報の保護と情報流通の活性化を図る個人情報流通管理方法に関するものである。

【0002】

【従来の技術】インターネット上でオンラインショッピングや電子商取引を行う際は、認証、顧客管理、マーケティング、配達先情報などの必要性から利用者の個人情報の入力が必要であった。利用者は商品購入やサービス提供を受ける度に個人情報の入力を要求され、同じような情報を入力しなければならなかった。その煩わしさに加え、提供した自分の個人情報が、どこでどのように使用されているのか、また、知らないところで公開、流通されたりしないのかという不安があった。

【0003】上記問題を解決するための技術としては、World Wide Web Consortium(W3C)でWorking Draftとして検討中のPlatform for Privacy Preferences(P3P)(<http://www.w3c.org/P3P/>)などがある。P3PはWebサイトを訪れた利用者の個人情報に対して、開示／拒否／拒否の場合の代替条件を設定することで個人情報の保護を可能にしている。具体的には、Webサイトが個人情報を入手する時、取得したい個人情報の項目、利用目的や開示する範囲などをWebサイトのプライバシーに関する要求として利用者に明示し、利用者はその説明内容に応じて、個人情報の開示に合意／拒否／代替条件を採用するか選択することができる。Webサイトが予めプライバシーに関する要求を宣言し、利用者が個人情報のデータセットと開示のための条件設定を用意しておけば、Webサイトの要求と利用者の設定とを比較し、自動的に合意に至ることを可能にしている。また、合意に至らなくてもWebサイトが利用目的に応じて複数の要求を宣言していれば、別の要求に対して合意に至ることができる。さらに、Webサイトは利用者が訪れる度にプライバシーに関する要求を送らなくても、以前合意が取れたものに関しては、再取得の手間を省くことを可能にしているため、同じ情報を何度も入力する必要がない。

【0004】

【発明が解決しようとする課題】上記の従来技術では、個人情報の提供者(Webサイト訪問者)と個人情報の利用者(Webサイト)が合意に至っても、合意後に取得する個人情報のデータセット単体だけでは、利用権が明確に定義されなっていないのでWebサイトに対して、一度でも個人情報を公開すると、Webサイトがその情報を再利用するために保持したり、Webサイト間で情報を共有することを防ぐことができないという問題があった。また、取得した個人情報の譲渡など、個人情報の正当な二次利用については実施者(Webサイト)の判断に任されていたという問題がある。

【0005】本発明の目的は、個人情報利用主体に対し、個人情報を利用許諾情報で許可された範囲内での利用に制限することが可能な個人情報流通管理方法、装置、および個人情報流通管理プログラムを記録した記録媒体を提供することにある。

【0006】

【課題を解決するための手段】本発明の個人情報流通管理方法は、個人情報とその開示条件を規定した開示利用規定との組をデータベースに登録する個人情報登録段階と、前記データベースに登録された個人情報と開示利用規定の組の集合に対し、検索条件として与えられる個人情報の利用条件を規定した要求利用規定とに基づいて、開示利用規定と要求利用規定の両者の条件を満たす個人情報と開示利用規定とからなる組を検索する個人情報検索段階と、検索の候補となった個人情報と開示利用規定の組と、検索条件として与えられる要求利用規定とに基づ

づいて、開示済み個人情報と利用許諾情報を動的に生成し、開示済み個人情報と利用許諾情報を組にして個人情報利用主体に提示する個人情報提示段階とを有する。

【0007】本発明は、少なくとも1つの開示可能な個人情報を所持する個人情報所持主体と該個人情報所持主体から個人情報を開示して欲しい個人情報利用主体とが存在する情報流通基盤において、図5に示すように、個人情報所持主体は開示可能な個人情報のデータセットと該個人情報に対する利用制約を規定した開示利用規定とを組にして管理し、個人情報利用主体は要求する該個人情報についての利用条件を規定した要求利用規定を作成し、該開示可能な個人情報と該開示利用規定の組と個人情報利用主体から与えられる要求利用規定に基づいて検索を行い、個人情報利用主体に開示される開示済み個人情報と、該開示利用規定と該要求利用規定に基づいて導出される利用許諾情報とを組にして提示することで、個人情報利用主体に対し、該利用許諾情報で許可された範囲内での利用に制限することが可能となる。

【0008】また、本個人情報流通管理方法では、個人情報利用主体が、提示された該利用許諾情報で規定された範囲内で新たな開示利用規定を規定し、該開示済み個人情報と該新たな開示利用規定とを組にして管理することで、新たな個人情報所持主体となることができ、個人情報の正当な二次利用を実現可能とする。

【0009】また、本発明の個人情報流通管理装置は、データベースと、個人情報とその開示条件を規定した開示利用規定との組をデータベースに登録する個人情報登録手段と、前記データベースに登録された個人情報と開示利用規定とからなる組の集合に対し、検索条件として与えられる個人情報の利用条件を規定した要求利用規定に基づいて、開示利用規定と要求利用規定の両者の条件を満たす個人情報と開示利用規定とからなる組を検索する個人情報検索手段と、表示装置と、検索の候補となった個人情報と開示利用規定の組と、検索条件として与えられる要求利用規定とに基づいて、開示済み個人情報と利用許諾情報を動的に生成し、開示済み個人情報と利用

許諾情報と利用許諾情報を組にして前記表示装置に表示する個人情報提示手段とを有する。

【0010】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【0011】図1を参照すると、本発明の一実施形態の個人情報流通管理装置は個人情報入力装置1と個人情報登録部2とメモリおよび二次記憶装置3と検索条件入力装置4と個人情報検索部5と個人情報提示部6と表示装置7で構成されている。

【0012】個人情報所持主体は、少なくとも1つの開示可能な名前や住所や生年月日などの個人情報があった場合、個人情報入力装置1を用いて、これらを編集し、それに加えて個人情報の各項目について、利用許可者、利用目的、開示範囲などの開示条件を開示利用規定として作成する（ステップ11）。例えば、「名前はすべての人に任意の目的で開示する」ことを許し、「住所はユーザーサポートの目的であれば、〇〇株式会社に開示しても構わないが、開示範囲は個人情報利用主体の組織までとする」などである。

【0013】個人情報登録部2では、入力された個人情報と開示利用規定とからなる組を構文解析し、記述されている文章内容を読み取り、解析結果の情報をデータベースである二次記憶装置3に登録する（ステップ12）。この際、個人情報に関しては、個人情報の各項目や該項目のとり値を検索キーに検索ができるような索引を作成する。また、開示利用規定に関しては、開示対象となる個人情報の項目、利用許可者、利用目的、開示範囲などを検索キーにして検索ができるような索引を作成する。

【0014】個人情報利用主体は、検索条件入力装置4を用いて、表1に示すように、利用したい個人情報の項目ごとに、利用目的、開示範囲などを要求利用規定として作成し、個人情報検索部5へ送る（ステップ13）。

【0015】

【表1】

開示対象の個人情報の指示子	利用許可者	利用目的	開示範囲
個人情報ID+名前	任意の人	無制限	再配布可能
個人情報ID+自宅住所	△△商事以外	ユーザーサポート	あなたの組織
個人情報ID+自宅電話番号	同じ職場の人	個人利用	あなたのみ
個人情報ID+職場電話番号	任意の人	マーケティング	あなたの組織
個人情報ID+職場電子メールアドレス	or.jpドメインの人	非営利	あなたのみ

【0016】個人情報検索部5では、登録されている開示利用規定の条件と検索条件として与えられた要求利用規定の条件とを索引を用いて照らし合わせ、両者の条件を満たす個人情報と該開示利用規定とからなる組を検索する（ステップ14）。

【0017】このとき、開示利用規定の中に異なる情報利用主体ごと、または開示条件ごとに、開示する個人情報を複数定義している場合、個人情報の選択開示が可能

である。例えば、「自分と同じ会社の人には、自宅電話番号として電話番号1を開示し、その他の人には、電話番号2を開示する」や「ユーザーサポートの目的であれば、職場電子メールアドレスとして、メールアドレス1を開示するが、ダイレクトメール送付の目的の場合は、メールアドレス2を開示し、営利目的の場合は、開示しない」などを規定することが可能である。

【0018】個人情報提示部6では、検索結果に基づ

き、開示する個人情報の項目を抽出することにより、開示済み個人情報を動的に作成し、これに加えて、該開示済み個人情報の各項目に対して、開示利用規定と要求利用規定に基づいて利用許諾情報を動的に生成し、開示済み個人情報と利用許諾情報を組にして管理し、表示装置7に表示する(ステップ15)。

【0019】この利用許諾情報は、上述した開示利用規定の条件と要求利用規定の条件との両者を満たす利用制約となっており、利用制約対象となる個人情報の項目、利用許可者、原著作者、利用目的、開示範囲などが規定されている。個人情報利用主体が入手した個人情報は、必ずこの利用許諾情報との組で管理されるため、原著作者(個人情報所持主体)の意図に反した不正な利用を制限することができる。

【0020】また、利用許諾情報中に「開示済み個人情報の再配布」が許可されている場合、個人情報利用主体は、利用許諾情報で許可された範囲内で新たな開示利用規定を個人情報入力装置1から入力することで、個人情報所持主体になることができる。

【0021】なお、開示可能な個人情報と開示利用規定とからなる組の集合を登録したサーバーサイトが複数、分散して存在し、それらに対して検索要求を並行して送ることができるような構成とすることも可能である。

【0022】また、個人情報利用主体として、様々なサーバーサイトに登録された多数の個人情報所持主体から、再配布可能な開示済み個人情報を取得し、それらの利用許諾情報に規定された範囲内において、索引などを作成し、他の個人情報利用主体に対して、要求する個人情報はどのサーバーサイトに問い合わせをすると効率が良いかを案内したり、検索の代行を行ったりするサービスを提供することも可能である。

【0023】図3を参照すると、本発明の他の実施形態の個人情報流通管理装置は入力装置21と記憶装置22、23と表示装置24と記録媒体25とデータ処理装置26で構成されている。

【0024】入力装置21は例えばキーボードで、図1中の個人情報入力装置1と検索条件入力装置4に相当する。記憶装置22は図1中のメモリおよび二次記憶装置3に相当する。記憶装置23はハードディスクである。表示装置24は図1中の表示装置7に相当する。記録媒体25は図1中の個人情報入力装置1と個人情報登録部2と検索条件入力装置5と個人情報検索部5と個人情報提示部6の各処理からなる個人情報流通管理プログラムを記録した、FD(フロッピー・ディスク)、CD-ROM、MO(光磁気ディスク)等の記録媒体である。データ処理装置26は記録媒体25から個人情報流通管理プログラムを読み込んで、これを実行するCPUである。

【0025】図4は図1の個人情報流通管理装置を用いて情報サービス提供を行う装置の構成図である。

【0026】サービス提供主体(個人情報利用主体を含む)は、提供するサービスに応じて、該サービスを実施するために必要となるサービス利用主体(個人情報所持主体を含む)の個人情報と該個人情報の利用内容をサービス条件入力装置8から入力する。

【0027】ここでのサービスとは、サービス利用主体の趣味や嗜好、住所や年齢、性別などの個人情報に応じて、サービス提供主体が提供するサービスの内容や提供方法、提供頻度などが変わる個人適用型サービスなどのことである。

【0028】サービス条件入力装置8から入力された情報に基づき、要求利用規定生成部9で要求利用規定を生成し、生成した該要求利用規定を個人情報検索部5へ入力する。個人情報検索部5は、要求利用規定に応じて、前記検索処理を行い、個人情報提示部6はサービス利用主体の開示済み個人情報と利用許諾情報とからなる組をサービス提供判定部10に提示する。サービス提供判定部10は、サービス利用主体に対して、該サービスを実行するのに必要な個人情報が得られたかどうか、また得られた個人情報に対する利用許諾情報の利用目的や開示範囲が該サービスを実行するために必要な条件を満たしているかどうかを判定する。判定の結果、該サービスの実行が可能であれば、サービス提供主体は、サービス利用主体に対し、サービスの提供を行う。

【0029】本実施形態では、サービス提供主体がサービス利用主体の開示済み個人情報と利用許諾情報とからなる組を要求する構成としたが、サービス利用主体があらかじめ開示済み個人情報と利用許諾情報をサービス提供主体に提示、登録しておき、サービス提供主体が提供可能なサービスが発展した時点で、サービス利用主体にサービスを行う構成とすることもなども可能である。

【0030】また、サービス条件入力装置8、要求利用規定生成部9、個人情報検索部5、個人情報提示部6、サービス提供判定部10からなる処理も、図3の実施形態と同様に、FD、CD-ROM、MO等の記録媒体に記録して、パソコン等のコンピュータで実施できる。

【0031】

【発明の効果】以上説明したように、本発明によれば、下記のような効果がある。個人情報所持主体の意図に反した個人情報利用主体の不正な利用を制限できる。また、個人情報利用主体が新たに個人情報所持主体になることで正当な個人情報の二次利用が可能になる。また、個人情報所持主体は、オンラインショッピングなどの際に、何度も同じ情報を入力する手間が省ける。さらに、相手に応じて開示する個人情報を選択開示することが可能になるなど、個人情報の保護と情報流通の活性化を両立させることができる。

【図面の簡単な説明】

【図1】本発明の一実施形態の個人情報流通管理装置の構成図である。

【図2】図1の個人情報流通管理装置の全体の処理の流れを示すフローチャートである。

【図3】本発明の他の実施形態の個人情報流通管理装置の構成図である。

【図4】図1の個人情報流通管理装置を用いた情報サービス提供装置の構成図である。

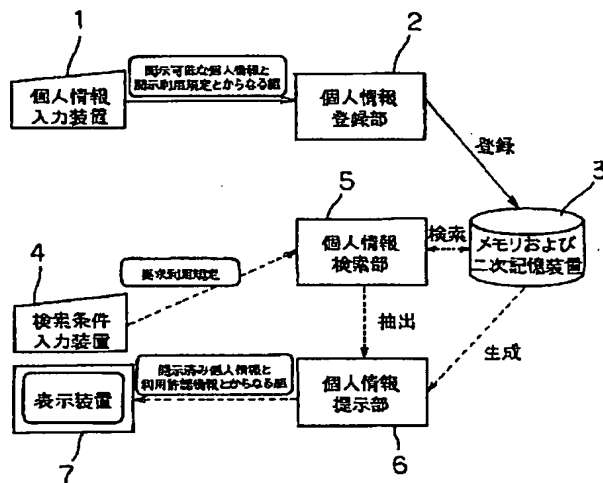
【図5】個人情報所持主体と個人情報利用主体とが存在する情報流通基盤を示す図である。

【符号の説明】

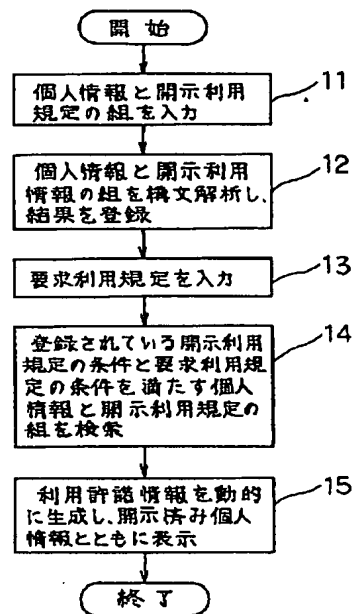
- 1 個人情報入力装置
- 2 個人情報登録部
- 3 メモリおよび二次記憶装置
- 4 検索条件入力装置

- 5 個人情報検索部
- 6 個人情報提示部
- 7 表示装置
- 8 サービス条件入力装置
- 9 要求利用規定生成部
- 10 サービス提供判定部
- 11～15 ステップ
- 21 入力装置
- 22、23 記憶装置
- 24 表示装置
- 25 記録媒体
- 26 データ処理装置

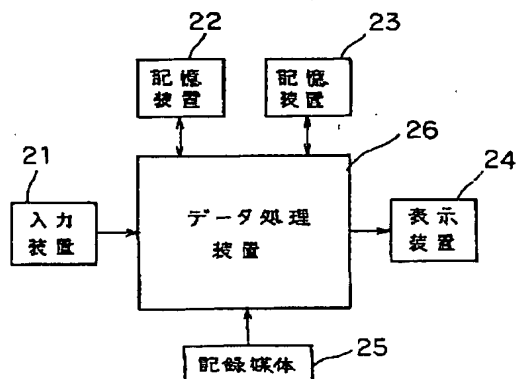
【図1】



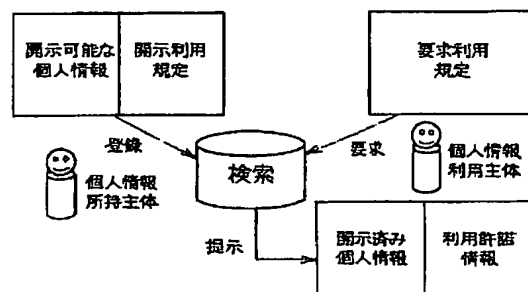
【図2】



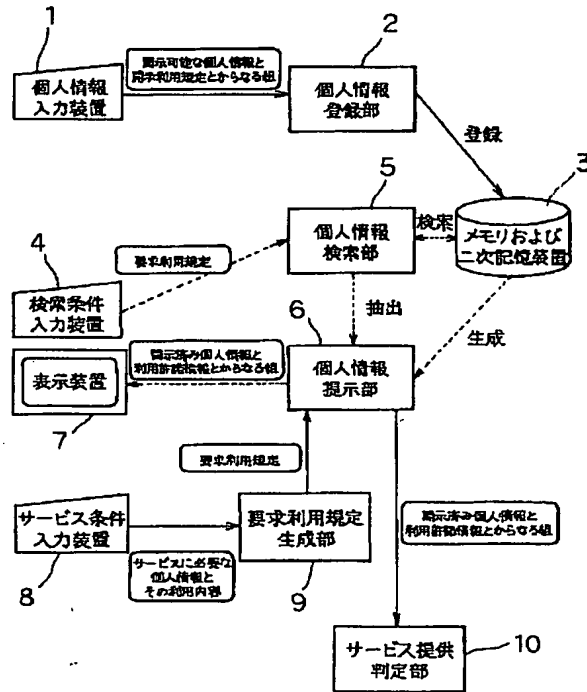
【図3】



【図5】



【図4】



フロントページの続き

(72) 発明者 梅本 佳宏  
東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内

(72) 発明者 佐藤 哲司  
東京都千代田区大手町二丁目3番1号 日  
本電信電話株式会社内  
Fターム(参考) 5B075 KK43 KK54 UU08  
5B085 AE06 BE07